

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Jan van Aken, Herbert Behrens, Steffen Bockhahn, Christine Buchholz, Annette Groth, Ulla Jelpke, Harald Koch, Niema Movassat, Jens Petermann, Paul Schäfer (Köln), Dr. Petra Sitte, Frank Tempel, Kathrin Vogler, Halina Wawzyniak, Katrin Werner und der Fraktion DIE LINKE.

„Strategische Fernmeldeaufklärung“ durch Geheimdienste des Bundes

Das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) dürfen den elektronischen Datenverkehr unter anderem im Rahmen der Terrorabwehr durchforsten. Ähnliches gilt für das Zollkriminalamt (ZKA), das auch entsprechende nachrichtendienstliche Befugnisse hat. Am 25. Februar 2012 berichtete die „Bild“-Zeitung unter Berufung auf zwei Berichte des Parlamentarischen Kontrollgremiums (PKGr) des Deutschen Bundestages, dass im Jahr 2010 mehr als 37 Millionen E-Mails und Datenverbindungen von den deutschen Geheimdiensten überprüft wurden, weil darin bestimmte Schlagwörter wie „Bombe“ vorkamen. Damit hätte sich die Zahl im Vergleich zum Vorjahr mehr als verfünffacht. Nach PKGr-Angaben ergaben die Überwachungsmaßnahmen insgesamt nur in 213 Fällen verwertbare Hinweise für die Geheimdienste.

Das PKGr schreibt in seinem Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes (Bundestagsdrucksache 17/8639), dass 2010 die Behörden in E-Mails und anderen Kommunikationen nach rund 16 400 Begriffen gesucht hätten. Der größte Teil (rund 13 000) entfiel dabei auf den Bereich des Waffenhandels; dort wurden auch mit 25 Millionen die meisten Gespräche und Mail-Konversationen erfasst. Davon wurden letztlich jedoch nur 180 als „nachrichtendienstlich relevant“ eingestuft; „hierbei handelte es sich um 12 E-Mail-, 94 Fax- und 74 Sprachverkehre“, heißt es in dem Bericht. Das PKGr führt das Verhältnis zwischen Aufwand und Erfolg unter anderem auf das Spam-Aufkommen zurück: „Die zur Selektion unerlässliche Verwendung von inhaltlichen Suchbegriffen, bei denen es sich auch um gängige und mit dem aktuellen Zeitgeschehen einhergehende Begriffe handeln kann, führt unweigerlich zu einem relativ hohen Spam-Anteil, da viele Spam-Mails solche Begriffe ebenfalls beinhalten können“. Es liegt nahe, dass Wörter, Satzteile oder Phoneme gleicher Bedeutung parallel in mehr als einer Sprache verwendet werden.

Nach Angaben von PKGr-Mitgliedern handle es sich bei der Maßnahme nicht um eine Rasterfahndung im Telekommunikationsverkehr bestimmter deutscher Bürger in Deutschland, sondern um eine „strategische Überwachung der gebündelten Funkübertragung etwa über asiatischen oder afrikanischen Ländern“. Deutsche dürften hiervon kaum betroffen sein. Falls doch, gelte für sie prinzi-

piell der Schutz des Grundgesetzes mit der Pflicht zur sofortigen Datenlöschung. Über die Zulässigkeit und Notwendigkeit der Anordnung einschließlich der Verwendung von Suchbegriffen entschieden die im PKGr vertretenen unabhängigen Fachleute (vgl. heise.de vom 27. Februar 2012).

Das PKGr schreibt in seinem Bericht: „Strategische Kontrolle bedeutet, dass nicht der Post- und Fernmeldeverkehr einer bestimmten Person, sondern Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, nach Maßgabe einer Quote insgesamt überwacht werden. Aus einer großen Menge verschiedenster Gesprächsverbindungen werden mit Hilfe von Suchbegriffen einzelne erfasst und ausgewertet“. Nach Ansicht der Fragesteller und Angaben von Experten müssen die Geheimdienste jedoch, wenn sie bestimmte Suchbegriffe in E-Mails finden wollen, jede E-Mail filtern. Technisch bedient man sich hierbei einer „Parsing“ genannten Syntanalyse.

Wir fragen die Bundesregierung:

1. Inwieweit werden neben Internetverkehr, E-Mails, Faxverbindungen, Webforen und Sprachverkehren durch deutsche Geheimdienste weitere Kommunikationskanäle im Rahmen der „strategischen Fernmeldeaufklärung“ ausgespäht?
 - a) Auf welche Art und Weise wurden die „12 E-Mail-, 94 Fax- und 74 Sprachverkehre“ im Bereich „Proliferation und konventionelle Rüstung“ sowie die „7 Metadatenerfassungen, 17 Webforenerfassungen und 5 Sprachverkehre“ im Bereich „Internationaler Terrorismus“ erhoben (Bundestagsdrucksache 17/8639)?
 - b) Was ist mit der „Metadatenerfassung“ gemeint, und auf welche Art und Weise wird diese vorgenommen?
 - c) Welche weiteren sechs Kommunikationsverkehre wurden im „Gefahrenbereich ‚Illegale Schleusung‘“ neben ausspionierten E-Mails erfasst?
2. Nach welchem technischen Verfahren werden die Kommunikationsverkehre durchforstet?
 - a) Trifft es zu, dass der BND, der MAD und das BfV sowie das ZKA hierfür Software der Firmen trovicor GmbH, Utimaco AG, Ipoque GmbH oder ATIS UHER einsetzen, und falls ja, um welche konkreten Anwendungen handelt es sich?
 - b) Wenn nicht, von welchen Firmen oder welcher Firma stammt die eingesetzte Software?
 - c) Handelt es sich dabei um ein Parsing, Tagging, einen Stringvergleich oder andere Verfahren der Zuordnung von Wortklassen?
 - d) Wie viele Mitarbeiter sind jeweils mit der Durchführung dieser Maßnahme betraut?
3. Ist die eingesetzte Technik auch in der Lage, verschlüsselte Kommunikation (etwa per Secure Shell oder Pretty Good Privacy) zumindest teilweise zu entschlüsseln und/oder auszuwerten?
4. Wie hoch sind die Kosten für die Kommunikationsüberwachung im Rahmen der „strategischen Fernmeldeaufklärung“, aufgelistet nach
 - den Kosten für die Anschaffung der technischen Ausrüstung,
 - den laufenden Kosten für die technische Ausrüstung,
 - den Personalkosten und
 - den sonstigen Kosten?

5. Auf welche Art und Weise werden die „Stichproben“ der „strategischen Fernmeldeaufklärung“ bestimmt?
 - a) Was ist mit der „Maßgabe einer Quote“ gemeint, nach der „Gesprächsverbindungen“ – laut Bundestagsdrucksache 17/8639 – ausgespäht werden?
 - b) Nach welchen Kriterien werden die Rasterungen gemäß dieser „Quote“ vorgenommen?
6. Wie wurden die 16 400 Begriffe, nach denen die Kommunikation durchforstet wird, bestimmt?
 - a) Welche Abteilung ist hierfür jeweils zuständig?
 - b) Auf welche weiteren Analysen welcher weiteren Behörden oder Institutionen wird dabei zurückgegriffen?
7. Wie viele TK-Verkehre (TK = Telekommunikation) werden bzw. wurden tatsächlich gefiltert, um auf die angegebenen Zahlen zu kommen (bitte nach E-Mails, Fax- und Sprachverkehren aufschlüsseln)?

Sofern keine Angabe zur konkreten Zahl möglich sein soll, in welcher Größenordnung bewegt sich die Zahl?
8. Wurden die tatsächlich gefilterten und/oder erfassten TK-Verkehre protokolliert?
 - a) Wenn ja, wer ist berechtigt, diese Protokolle auszuwerten, und zu welchem Zweck?
 - b) Welche Informationen werden protokolliert?
9. Werden bei der „strategischen Fernmeldeaufklärung“ Kommunikationsverkehre lediglich von und nach Deutschland ausgespäht?
 - a) Falls nein, wie viele der überwachten Kommunikationsverkehre bezogen sich auf Verbindungen ins Ausland?
 - b) Falls ja, wie wird bei der strategischen Auswertung von E-Mails zwischen rein inländischen und Verkehren aus dem und in das Ausland unterschieden, insbesondere dann, wenn der E-Mail- oder Weblog-Provider keine „.de“-Adresse verwendet bzw. der Server im Ausland steht?
 - c) Was versteht die Bundesregierung unter „Webblog-Kommunikation“?
 - d) Inwieweit wird bei der „Webblog-Kommunikation“ bestimmt, ob es sich dabei nicht um eine „innerdeutsche“ Kommunikation handelt?
 - e) Inwieweit werden Kommunikationsverkehre auch nach den Adressen bzw. Telefonnummern der Absender (Absenderkennung) oder Adressaten (Zielkennung) gefiltert?
10. Inwieweit wird unterschieden, ob ein Kommunikationsverkehr für die weitere Beobachtung oder Strafverfolgung relevant ist?
 - a) Werden auch firmeninterne Kommunikationsverkehre überwacht, indem etwa E-Mails zwischen gleichen Domains ausgespäht werden?
 - b) Inwieweit wird sichergestellt, dass Abgeordnete, Rechtsanwältinnen/Rechtsanwälte, Journalistinnen/Journalisten oder Diplomaten von den Spionagemassnahmen ausgeschlossen werden?

11. Auf welche Art und Weise und wie lange wurden bzw. werden die Kommunikationsverkehre für die Auswertung gespeichert oder kurzzeitig vorgehalten?
 - a) Auf welche Art und Weise werden gefundene „Treffer“ weiter bearbeitet?
 - b) Wo werden vermeintliche „Treffer“, also Kommunikationsverkehre mit „verdächtigem“ Vokabular weiter gespeichert, und wer hat darauf Zugriff?
 - c) Wie lange bleiben die TK-Verkehre bei diesem Prozess (ggf. auch nur in einem temporären Speicher) gespeichert (bitte nach E-Mails, Fax- und Sprachverkehren aufschlüsseln)?
 - d) Wie ist der Umgang mit nicht relevanten, aber erfassten TK-Daten?
 - e) Wie viele der erfassten TK-Verkehre waren unbrauchbar auf Grund von „Spam“?
12. Inwieweit werden Kommunikationsverkehre auch durch die Auswertung gesprochener Wörter ausgespäht?
 - a) Werden Wörter bzw. Satzteile oder Phoneme gleicher Bedeutung parallel in mehr als einer Sprache als Suchbegriff verwendet?
 - b) Welche Abteilungen bei BND, MAD und BfV sind zuständig für die Entwicklung von Systemen zur Spracherkennung?
13. Worauf stützt die Bundesregierung die Behauptung, der Anstieg der überwachten Kommunikationsverkehre sei dem steigenden Versand von Spam-E-Mails geschuldet, obschon dieser im fraglichen Zeitraum laut anderen Statistiken eher zurückgegangen war?
14. In wie vielen Fällen waren die erlangten „Erkenntnisse“ ermittlungsrelevant oder trugen wesentlich zur Aufklärung oder Abwehr schwerer Straftaten bei?
 - a) Sofern hierzu keine Statistiken mitgeteilt werden können, in welcher Größenordnung bewegen sich etwaige „positive“ Ergebnisse?
 - b) Wie verteilten sich die gefundenen Treffer auf die Kriminalitätsphänomene „Bewaffneter Angriff auf die Bundesrepublik Deutschland“, „Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland“, „Internationale Verbreitung von Kriegswaffen“, „Unbefugte gewerbs- oder bandenmäßig organisierte Verbringung von Betäubungsmitteln“, „Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen“, „International organisierte Geldwäsche“, „Gewerbsmäßig oder bandenmäßig organisiertes Einschleusen von ausländischen Personen“?
15. Durch welche weiteren Maßnahmen nehmen BND, MAD und BfV ihre gesetzlichen Aufgaben zur Überwachung des Telekommunikationsverkehrs wahr?
16. An welchem Ort stehen die vom BND genutzten Informationssysteme bzw. die zur „strategischen Fernmeldeaufklärung“ genutzte Hardware?
 - a) Inwieweit greifen Bundesbehörden zur Überwachung von Telekommunikation auf den Verkehr über den Frankfurter Netzknoten DE-CIX (German Commercial Internet Exchange) zu?
 - b) Inwieweit arbeiten Bundesbehörden zur „strategischen Fernmeldeaufklärung“ auch mit den kommerziellen Telekommunikationsprovidern zusammen?

17. Inwieweit wird für die Überwachung von internationalen Telekommunikationsverbindungen auf die Verbindungsstellen zum Ausland (die sogenannte Auslandskopfüberwachung) zugegriffen?

Wie viele „Auslandsköpfe“ werden nach Kenntnis der Bundesregierung bzw. der Regulierungsbehörde für Telekommunikation und Post von welchen Netzbetreibern betrieben?

18. Gilt das Briefgeheimnis aus Sicht der Bundesregierung auch für elektronische Kommunikation?

Falls ja, wie wird dann die „vorsorgliche“ Spionage elektronischer Kommunikation gegenüber herkömmlichem Briefverkehr abgegrenzt, der ja nicht anlasslos ausgeforscht wird?

19. Welches sind die im PKGr vertretenen unabhängigen Fachleute?

a) Wer benennt diese Fachleute?

b) Auf welcher Grundlage wurden diese Fachleute ausgewählt?

20. Kann die Bundesregierung anhand ausgewählter „Treffer“ illustrieren, ob es sich bei der „strategischen Fernmeldeaufklärung“ tatsächlich um ein sinnvolles Instrument zur Feststellung schwerer Straftaten handelt?

Berlin, den 5. April 2012

Dr. Gregor Gysi und Fraktion

